18th ICCRTS
"C2 in Underdeveloped, Degraded and Denied Operational Environments"

Title of Paper
Impact of Trust on Security and Performance in Tactical Networks

Topic Topic 1: Concepts, Theory, and Policy

Name of Author(s)
Kevin Chan, US Army Research Laboratory
Jin-Hee Cho, US Army Research Laboratory
Ananthram Swami, US Army Research Laboratory

Point of Contact
Kevin Chan
RDRL-CIN-T
2800 Powder Mill Rd.
Adelphi, MD 20783
kevin.s.chan@us.army.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Impact of Trust on Security and Performance in Tactical Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Research Laboratory,RDRL-CIN-T,2800 Powder Mill Rd.,Adelphi,MD,20783**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 19-21 June, 2013 in Alexandria, VA.

14. ABSTRACT
Traditional approaches to networking and security operate with static metrics with a blackand- white approach towards decision-making. With the advent of network centric environments and the emerging consideration of the impact of social networks on communication networks, we are forced to better understand how these additional factors can be used to improve networking services without assuming an unacceptable amount of risk. We have considered the implemen- tation of trust metrics into various network protocols and security services. Our trust metric considers the impact of parameters of communication, information and social networks. Using these parameters, we have developed composite trust metrics and applied them to the decision- making process within these protocols to replace the traditional approaches. Using trust-based approaches, the goal is to allow these protocols to operate in the gray area to improve perfor- mance and the range of operating conditions. We have studied tradeoffs between performance and security and trust and risk to identify optimal operating conditions of networks to maximize performance in several networking applications.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**31**	

Abstract

Traditional approaches to networking and security operate with static metrics with a *black-and-white* approach towards decision-making. With the advent of network centric environments and the emerging consideration of the impact of social networks on communication networks, we are forced to better understand how these additional factors can be used to improve networking services without assuming an unacceptable amount of risk. We have considered the implementation of trust metrics into various network protocols and security services. Our trust metric considers the impact of parameters of communication, information and social networks. Using these parameters, we have developed composite trust metrics and applied them to the decision-making process within these protocols to replace the traditional approaches. Using trust-based approaches, the goal is to allow these protocols to operate in the *gray* area to improve performance and the range of operating conditions. We have studied tradeoffs between performance and security and trust and risk to identify optimal operating conditions of networks to maximize performance in several networking applications.

1 Introduction

Tactical networks have been designed and operated with using traditional protocols procedures and policies, which offer little in the way of adaptability or flexibility. Given that the complexity of tactical environments is rapidly increasing, inflexible protocols and policies may prove to be incompatible with these networking environments. Current work is addressing the call for algorithms and policies to handle the dynamics and complexity of the tactical environment. Soldiers today are required to work in much more complex environments than in the past, where they previously may have only teamed with fellow Soldiers. Now, as part of counterinsurgency (COIN) operations, Soldiers must interact with individuals and systems from coalition organizations such as Soldiers of other nations, foreign nationals, and non-governmental agencies. The scope of tactical networks has increased to cover more than just the networked systems- it includes the associated individuals operating and those that come into contact with any part of the network. In addition, tactical networks also comprises the information and social/cognitive components of tactical environments.

As tactical operations become more net-centric, there is an increased reliance on the networks to provide Soldiers with valuable information and intelligence. Increasing the capability of information networks has been a dominating theme among tactical environments, with programs such as information superiority/dominance [1], data to decision [2], data fusion [3], and the global information grid [4]. The goals of these programs have been to find more adaptive and dynamic approaches to better accommodate the complexity of these tactical environments. These approaches typically aim to enhance agility, robustness, and resilience; by either maintaining performance in highly uncertain environments, or improving efficiency in normal operating environments. The Army Research Laboratory's Network Science Collaborative Technology Alliance (NS CTA) seeks to understand the

mathematical principles and laws that govern the co-evolution of the information, social-cognitive and communication networks [5]. The International Technology Alliance (ITA) on Network and Information Sciences, in which ARL is partnered with the UK Ministry of Defence (MoD), seeks to develop the basic theory behind coalition operations, both from a secure networking perspective as well as from a decision making one [6].

One of these approaches is to consider trust as a concept in the design and development of such network services. Using trust-based approaches to augment traditional networking methods allows one to exploit the multi-genre aspects of the problem. In this paper, we propose our current understanding of trust-based research applied to networks along with our opinions on the benefit of using trust in tactical networks.

In this paper, we propose to apply some ideas from trust-based research to networks along with our opinions on the benefit of using trust in tactical networks. The next section describes the motivation behind the use of trust in these applications. In Section 3, we describe the enhancements to networking and security services that trust may provide. In Section 4, we discuss our belief of the application of trust management systems in tactical networks. In addition, Section 4 address how trust can be modeled in a different domain and a multi-domain dealing with multi-genre networks. Section 5 describes two trust-based applications to tactical networks and a brief summary of the current research in these areas. Long-term goals and concluding comments are in Sections 6 and 7.

2 Trust in Tactical Networks

Trust has been defined many ways in the social sciences, but it is generally accepted that trust is the willingness of an entity to take a risk [7]. A trust relationship involves a trustor placing trust in a trustee even if the trustor may be betrayed by the trustee not behaving as expected. That is, the trust relationship implies a vulnerability or risk. We assume that the trustor may decide to interact with another node if its perceived trust in the other node is sufficient for the task and context. There has been a wide range of trust research proposing various models to characterize trust. While obvious connections to tactical networks, there has been a great deal of work done with regard to trust in automation and human machine interaction [8, 9]. While these concepts primarily have developed in the social sciences, the challenge is to apply trust into tactical networks in a meaningful and beneficial way across the communication networks and personnel/organizations consumed in the tactical network paradigm.

In tactical networking situations, trust may be present in a wide range of activities such as networking services, security services, and/or command and control (C2) scenarios. Networking services support the flow of information through the network in the form of data exploitation, processing or routing. In terms of security, trust may be used in typical security services such as authentication of identities, issuing of public keys, determination of information integrity, or participation in

secure routing. In terms of C2 perspective, trust is a key element involving interactions between non-homogeneous populations. This involves the handling information among coalition members; commanding teams and individuals or systems from varying backgrounds; or, COIN operations all of which require promoting trust in extreme situations with high uncertainty and risk.

We have two distinct uses of trust in these situations: human trust and computational trust. As a method to represent the tactical network in terms of a set of network layers, we consider three constituent network layers within a composite tactical network. The composite network is comprised of a communication, information, and social/cognitive network layer. In human trust, we aim to determine which policies, training, or other system parameters may be adjusted to enhance trust relationships - and ultimately performance - in tactical environments. These trust relationships ultimately lie in the social network layer. In terms of computational trust, we assume that this trust lies in the communication or information network layers, where agents are making decisions based on rules or some policies enforced by the system design. Trust in this case is controlled in order to support the potential of attaining global system goals such as agility, resilience, scalability, and survivability. Given that the concept of trust has roots in the social sciences, the complexity and scope and parameters and conditions that influence trust is countless. In this work, we consider models of several parameters and understand that this may not capture the entire characterization of the concept of trust. Our motivation is one to apply parts of the concept of trust to the modeling of different aspects of tactical networks to determine if these approaches may enhance the utility of such networks.

With these requirements and some preliminary investigations into the viability of using trust in tactical networks, several arguments against such claims have emerged with regard to the relationship of trust and tactical networks. This work examines the benefit of using trust in tactical networks in terms of four questions:

1. Can trust be defined in tactical networks?
2. Why is trust useful in tactical networks?
3. Can trust enhance traditional networking services with regard to security and performance? If so, how?
4. Can we validate trust in tactical networks?

The remainder of the paper proceeds to answer these questions by providing supporting arguments for why trust and/or trust management is needed and critical. We describe recent work in trust-based security applications that outperform traditional approaches.

As part of the U.S. Army Research Laboratory's research collaborative program, called Network Science Collaborative Technology Alliance (NS CTA), there are several ongoing research thrusts that aim to address trust in tactical networks. There is a specific research program called the Trust and

Distributed Decision Making Cross Cutting Research Initiatives (CCRI), where the main research goal is to *understand and characterize trust, security, and how they support distributed decisions*. Its research objectives are particularly focused on: (1) modeling and measuring trust from the perspective of the trustor, taking into account the interactions among different network layers; (2) characterizing predictors of trust and distrust; and, (3) and developing mathematical theories for the impact of trust on network evolution. Building upon results from this NS CTA and other related work, we make the following claims on current research points with regard to the impact of trust in three areas of tactical networks:

1. Trust can provide soft metrics to requirements to achieve both security and performance goals based on the tradeoff between trust and risk.

2. Concepts and properties of trust can be translated into existing networking concepts and may enhance traditional models.

3. Tactical networks are an increasingly complex environment. Trust is suitable means to handle interactions between different layers of a multi-genre network and gain understanding of these environments.

4. Trust can augment applications that span the tactical networking space.

3 Trust in Networks and Network Security

We have taken steps to consider the inclusion of trust to be a viable aspect of network services within the communication network domain. We have some evidence that points to the ability of trust management in this space to enhance the capability of these networks. By introducing soft metrics or trust-based approaches to traditional networking or security services, the resulting network may be more adaptable or resilient to a greater amount of scenarios that the network may encounter. The concept of trust may enhance existing networking or security metrics. There are obvious parallels to trust constructs and networking concepts; examples are shown in Table 1. Trust management includes all the processes involved with managing trust evidence or trust values of entities such as how trust is formed, aggregated, propagated, updated, revoked, and recovered (or repaired). Further, each of these trust processes has parallels in the traditional networking or security space. One challenge of multidisciplinary research is the redundancy of concepts, which once coordinated, may provide greater insights to the complex network space. This section shows how concepts within trust may be applicable to specific networks services. We discuss each component of trust management with a comparison in Table 1.

- *Trust Formation*: We assume that trust is established with a prior trust evaluation based on the observed characteristics of the trustee and the attitude of the trustor. Different trust

Trust Management Services	**Traditional Networking Services**
Trust Formation / Update / Propagation	Learning, Refresh
Trust Aggregation	Information / Decision Fusion
Trust Revocation	Access / Key Revocation
Trust Recovery / Repair	Re-entry

Table 1: Trust management services and related traditional networking services

dimensions will be applicable to specific tactical environments or situations. As discussed earlier (See Section 2), trust describes numerous aspects of an entity in various contexts. In tactical networks, this process is critical to network performance since trust dimensions allow for the setting of evaluation criteria thresholds of trustors. Our prior work considers several aspects such as availability, competence, integrity, willingness, cooperativeness, betweenness, proximity, and social connectedness [10, 11, 12].

- *Trust Update*: Trust may be updated during continuous interactions between entities, but it may decay in the absence of interactions. Depending on characteristics of network environments, trust can be updated periodically by directly observing a trustee or requesting indirect trust evidence from third parties who have direct experience with the trustee [11]. In a network environment without frequent interactions such as in delay tolerant networks (DTNs), other techniques can be used to enhance indirect interactions to update trust [13]. When entities try to interact with trustworthy entities, high trust relationships are formed between trustworthy nodes while trust decays further over time in untrustworthy relationships, leading to the *Matthew effect* (i.e., the rich get richer and the poor get poorer). In [11], an exponential decay is used, but other representations are admissible in the models.

- *Trust Propagation*: To share trust evaluations with other neighboring nodes in the network, it is necessary to appropriately propagate such information throughout the network in a timely manner. In addition, as trust information (or evidence) is propagated, we consider the tradeoff between resource consumption (e.g., communication overhead) and accuracy of measured trust (or trust bias) by entities in distributed environments [11]. A trust threshold may be used to identify a trustworthy next-hop node to forward trust information (or evidence). We discuss critical tradeoff issues of trust management in Section 4.

- *Trust Aggregation*: This addresses mechanisms to combine evidence of trust. Many trust management protocols aggregate direct trust evidence (i.e., observed behaviors, credentials) and indirect trust evidence (i.e., recommendations, reputation). Moreover, when considering indirect evidence from different parties, a trustor needs to aggregate them to assess trust fairly and accurately. Trust evidence is weighted by the trustworthiness of sources and screened with a

meaningful trust threshold to determine credibility of received trust evidence [10]. Additionally, when combining positive evidence with negative evidence, *Bayesian inference* is a well-known technique to incorporate evidence into estimated values of trust [14].

- *Trust Revocation*: Trust may be revoked when interactions between two parties causes one's trust to go below a certain threshold [15]. Trust revocation can be enforced based on the agreement of direct observers of a trustee, through a majority voting rule, which may minimize detection errors (i.e., false positives and negatives).

- *Trust Recovery (or Repair)*: Depending on a given network environment or context, trust may be recoverable or repaired, offering *forgiveness (or redemption)* [16]. Reestablishing trust relationships should consider possible risk, being betrayed by the trustee again(e.g., the trustee does not behave as expected even if given a second chance). Depending on the perceived risk, the trustor needs to decide whether to offer a second chance to the trustee that demonstrated untrustworthy behavior in the past.

4 Trust Management

This section briefly gives the basic definition of trust management and critical tradeoffs that should be considered in designing trust management mechanisms.

4.1 What is Trust Management?

Trust management has been studied by many disciplines. We discuss two main fields of trust management study: 1) information technology; and, 2) organizational theory. In information technology, Blaze et al. [17] first introduces the term *trust management* and identified it as a separate component of security services in networks. Also, he believed that trust management can provide a unified approach for specifying and interpreting security policies, credentials, and relationships. In other words, trust management in this field has been studied to assure automated operations against security and reliability. On the other hand, in organizational theory, trust management has viewed trust as a key factor to manage relationships that flourish within individuals, groups, organizations, society, and counties [18]. One example shows the positive impact of trust in that counties with people trusting each other have higher rates of economic growth. This perspective posits that less worry about risks will lead to new opportunities for innovation. However, the attitude towards risk must be different if the failure of trusting other entities introduces serious consequences, for example, casualties in battlefields or disaster/emergency rescue situations. This work mainly focuses on how to use trust in military tactical networks where whether to trust or not impacts system performance and security significantly, which may lead to even mission failure or success.

In tactical networks, a trustor can be a cognitive entity, often assumed to be a human (i.e., user or operator), or an intelligent agent who can think, decide, and have meaningful relationships with other entities. A trustee can be thought of as any entity, not necessarily a cognitive entity (i.e., human, machine, service, or representation of information). Relationships between entities often significantly impact decisions. Therefore, trust management techniques include all aspects of two or more entities interact to enhance relationships or improve performance. Considering the concept of trust as *the willingness to take a risk*, trust is viewed as part of risk management, emphasizing the need for authentication of identities in situations with high uncertainty and evaluating potential cooperation with unknown entities. However, the application of trust management has been extended from authentication to various communications and networking applications, including secure routing, intrusion detection, key management, access control, and other decision support mechanisms.

4.2 What are Tradeoffs in Managing Trust?

In designing trust management systems, we identify several critical tradeoffs that may optimize system performance. We discuss three key tradeoffs as follows:

- *Trust Accuracy vs. Resource Consumption*: Trust does not come for free. For entities to cooperate or collaborate, a sufficient level of trust must be established. This may require entities to interact to each other for an extended period of time. However, exchanging or collecting evidence to estimate trust in distributed environments requires resource consumption where resources are often scarce in tactical networks such as mobile ad hoc networks (MANETs) or wireless sensor networks (WSNs). Finding a balance between burdening the system and improving its performance is important to reap the benefit from trust management schemes.

- *Trust vs. Risk (or Security)*: As stated previously, trust is the willingness to take a risk or to be vulnerable by trusting a trustee. Trust requires trading off risk for performance [19]. That is, trust is formed through not only evidence (e.g., credentials, observations, experiences) but also a belief or attitude. In order to maximize system performance, using trust is a soft security approach while traditional security mechanisms are regarded as a hard approach. These approaches often require additional communication or computation overhead. Fine-tuning the required trust and acceptable risk results in a tradeoff, one can make to maximize system or mission performance in tactical networks. We discuss this further in Section 5.

- *Trust vs. Uncertainty*: While risk is described as an assumed potential loss that may be caused by uncertainty, we consider uncertainty to be distinct from risk, but is a state that is impossible to be exactly described [20]. That is, due to uncertainty that is not realized by a trustor, a trustor may be vulnerable in trusting a trustee even if a trustor perceives high confidence in the trustee's behavior. Under highly uncertain situations, a trustor still can trust a trustee but with low confidence due to lack of direct experience.

As we've claimed previously, trust can be estimated from different genres of network such as communication, information and social/cognitive networks. This allows trust management systems to consider unique characteristics of a given constituent network in order to enhance existing network models. Allowing trust to be modeled using aspects throughout the complex composite network allows for the study of the interplay between the different network layers. Now we discuss approaches to capture trust properly from a single network layer while suggesting methods to examine the interplay between different network layers to obtain a composite trust representation (considering multi-dimensions of trust) using evidence from each of the constituent layers.

4.3 Domain-Specific Trust Models

In this section, we discuss existing trust models that have been developed in the following three conceptual domains: communication, information, and social/cognitive domains.

- *Communication Network Domain*: This network layer of a network mainly considers trust associated with the communication medium (e.g., wireless/radio frequency channel) which includes connectivity, network congestion, and various network layer attacks. Examples of typical tactical communication networks include WSNs, MANETs, DTNs, and hybrid networks. Trust assessment should consider the dynamics of trust's nature that can be introduced by network changes due to node mobility, failure, or membership change in disadvantageous terrains in tactical environments. Besides the potential resource restrictions in the tactical environments challenges, these dynamics can hinder accurate and reliable trust evaluation of entities in the network [10], [11].

- *Information Network Domain*: Trust in information is often evaluated by the trustworthiness of the information source; along with the reciprocal relationship, an entity's trustworthiness may be evaluated by the trustworthiness of the information it provides. By checking the provenance (i.e., owner information) of the information, trust in the information can be estimated. We can find similar techniques in our prior work such as screening trustworthy recommendations obtained from trustworthy sources, evaluating quality of information (QoI) based on the information provider [13], or forwarding trustworthy information to trustworthy entities.

- *Social/Cognitive Network Domain*: Social scientists, physiologists, and neuroscientists have studied social trust, interpersonal trust, and cognitive trust. Sociologists and psychologists have examined key factors that affect social trust (e.g., friendliness, kindness, reciprocity, social tie) [16]. Physiologists and neuroscientists have investigated the impact of trust behavior on hormone levels [21]. The existing body of research on trust in the social and cognitive science domain is vast and is gradually being more understood by multidisciplinary research communities, such as within the NS CTA.

4.4 Multi-Domain Trust Models

Even if trust management or evaluation has studied in various disciplines, little work has examined the interplay between trust relationships of different domains. Alberts and Huber [22] explain that effective information sharing can be achieved by contributions of multiple domains such as social, cognitive, and information domains. For instance, QoI in the information domain can increase shared situation awareness (i.e., cognitive domain), resulting in collaboration across teams or coalition partners (i.e., social domain). In addition, we notice the impact of communication network behaviors (e.g., quality of service - QoS) on QoI (e.g., freshness due to low delay, correctness due to reliable communication). All of these processes have the same goal, achieving high mission effectiveness. For example, we have recently studied the impact of communication network behavior (e.g., delay, connectivity) on cognitive trust [23]. The flaws in the communication network result in a biased estimation of the trust in other entities in the network; which ultimately leads to degradation in mission performance metrics.

Multi-domain trust models should be understood in terms of interactions or interplay between different network layers in a composite network even if each network layer needs to capture trust considering its own unique characteristics. To this end, diverse dimensions of trust should be considered to derive the so called *composite trust*.

5 Applications of Trust Management

In terms of applying these trust management concepts to different layers of the tactical network, we describe trust approaches applied to security services and to a C2 scenario. Security services mainly fall into the communication and information layers and command and control scenario concerns the communication and social network layers.

5.1 Trust-based Security Applications

Trust management has been employed to achieve security goals such as availability, confidentiality, authentication (or authorization), integrity, and non-repudiation. In the literature, diverse trust-based security applications have been proposed such as secure routing, intrusion detection, access control, and key management [1]. However, most studies use a single trust dimension (e.g., reliability or QoS) to measure trustworthiness of entities in networks.

We have proposed composite trust models and employed them for the following security purposes: secure routing [10], intrusion detection [24], and key management [25]. This shows preliminary impact of trust into network security problems. First, in secure routing, trust has introduced efficiency by using only trustworthy entities for routing and effectiveness for decision making by considering credible information. To be specific, Chen et al. [10] proposed a trust-based secure routing protocol for DTNs

based on both QoS trust and social trust to assess a node's trustworthiness. Since DTNs do not guarantee any end-to-end connectivity, message delivery can be significantly delayed. We use two trust thresholds: (1) a trust threshold to determine whether a next message carrier is trustworthy; and (2) a trust threshold to determine whether a received recommendation is credible based on the trust level of the recommender. They help assure accurate trust evaluation and high message delivery ratio by using trustworthy nodes as next message carriers and utilizing credible recommendations from trustworthy nodes. A trust threshold is used to screen trustworthy recommendations as trust evidence from trustworthy recommenders, leveraging the interdependency between trustworthiness of information and that of the information provider. Another trust threshold is used to select a trustworthy next message carrier to ensure reliable message delivery. For intrusion detection, an optimal trust threshold is identified to minimize false positives and negatives in identifying malicious entities. Bao et al. [24] developed a trust-based intrusion detection mechanism using a minimum trust threshold to determine a malicious node in a WSN. This work identifies an optimal minimum trust threshold that minimizes false positives and false negatives and showed the performance gain of the proposed scheme, compared to existing non-trust-based schemes. This work also shows how social trust (measured based on a node's integrity trust) affects detection performance. In addition, we have applied trust concept in a public key management application and showed how an optimal trust threshold for key generation, distribution, and revocation can maximize system goals such as security and performance. Cho et al. [25] proposed a distributed public key management protocol for MANETs using the composite trust metric. Similarly, this work also examined an optimal level of trust threshold under a various range of hostile network environment in order to determine who can generate and distribute its public key, whom to distribute the public key, and whom to provide a public key upon the receipt of the public key request. In trust-based security mechanisms, the trust threshold for decision making processes is critical to vulnerabilities to both security and performance. If a very low trust threshold is used for trust decisions (i.e., whether to trust or not), an entity is more likely to trust other entities, accordingly exposing security (or risk) vulnerability but opening prospective opportunities. In contrast, if a very high trust threshold is used for trust decision, an entity is less likely to trust other entities, leading to loss of gain or opportunities of prospective collaboration or cooperation that affects performance, instead of minimizing security vulnerability. Identifying an optimal trust threshold for trust decision is vital in order to achieve both security and performance in networks.

5.2 Trust-based Information Sharing in Command and Control

In considering trust in C2 scenarios, trust resides in the social network with communication and information networks impacting social relationships. Trust management takes on a form different from those considered in applications to security services. Here, humans are the entities making decisions on whether to share or believe information it possesses while performing alongside automated systems.

The performance of C2 scenarios are typically predicated on the ability of the network to promote the flow of information to enable decision makers to attain a sufficient level of situation awareness (SA).

In this application of trust, it is necessary to develop reasonable models of composite trust in order to formulate how trust may evolve over time and a series of interactions with other nodes in the network. Additionally, models of individual behavior can determine interaction models of nodes who may work together in certain C2 scenarios. Based on the trust evolution model and behavior models, we will be able to determine how organizations perform with certain collections of people and other network parameters such as connectivity and scalability. Characterization of these phenomena within representative scenarios will enable the prediction of performance and also allow for the control of networks to maximize SA and decision making ability in C2 networks.

We have ongoing work that defines a composite trust model for a specific C2 scenario, which is based on a experimental platform called Experimental Laboratory for Investigating Collaboration, Information-sharing, and Trust (ELICIT) [26]. ELICIT is an environment designed for either human or software agent participants to execute a information sharing task. With regard to an agent model of trust, we developed a composite trust model based on three factors: willingness, competence and intent [14]. Based on evaluations of the trustees, the trustor node is able to modify its behavior to attempt to maximize its own and the global performance. In this scenario, global performance is measured by attaining SA quickly and efficiently. We claim that the trust enhances the capability of the network to achieve these global system goals. In [14, 12], we show that the use of trust to determine interactions between nodes increases situation awareness gained by 30% at the cost of some communications overhead. The approach also maintains performance in the presence of misbehaving nodes as opposed to the case where trust was not considered.

6 Long-Term Goals

Despite being in the beginning stages of this research area, there are several long-term goals that would confirm the benefit of trust in tactical networks:

- Trust-based security services that use soft-metrics, but provide equivalent or enhanced security and performance
- Methods to promote trust, control trust within populations.
- Models across multi-genre networks that enable prediction of performance metrics.
- Validation of the models with operational scenarios using actual systems and human entities in the loop.

Availability of these tools would enhance the effectiveness of tactical networks.

7 Conclusion

In this paper, we discussed how trust can play a critical role in improving mission performance for tactical networks where resources are constrained and net-centric operations should be implemented in a distributed manner. We reviewed how trust can be defined, measured, propagated, updated, revoked, and repaired in a tactical network environment consisting of complex and diverse layers of networks. In addition, we addressed what critical tradeoffs exist and how the tradeoff between trust (or performance) and risk (or security) have been addressed in our prior work [7, 10, 11, 13, 25, 27]. Finally, we also showed how the so called *composite trust metrics* have been applied in various types of tactical applications. Due to the inherent nature of the concepts associated with trust such as subjectivity, validating trust models characterized by multiple trust dimensions from machine reliability to human trust is a challenge. As the first step to tackle this problem, we suggest modeling tactical missions (or tasks) properly in order to reflect key goals of tactical network environments by reflecting objectives from different layers of networks (i.e., communication, information, and social/cognitive networks) in developing the composite trust metric.

References

[1] D. S. Alberts, J. J. Garstka, R. E. Hayes, and D. A. Signori, *Understanding Information Age Warfare*. CCRP Publication Series, 2001.

[2] C. Schwartz, "Data-to-decisions S & T priority initiative," *NDIA Disruptive Technologies Conf.*, 2011.

[3] D. Hall and J. Llinas, *Handbook of Multisensor Data Fusion*. CRC Press, 2001.

[4] J. Tarr and T. DeSimone, "Defining the GIG core," *IEEE Military Communications Conf.*, pp. 1–6, 2007.

[5] "ARL Network Science Collaborative Technology Alliance." `http://www.ns-cta.org/`, Apr. 2013.

[6] "International Technology Alliance Collaboration System." `https://www.usukita.org/`, Apr. 2013.

[7] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[8] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, May 2000.

[9] J. D. Lee and K. A. See, "Trust in automation: Designing for appropriate reliance," *Human Factors*, vol. 46, pp. 50–80, 2004.

[10] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Integrated social and QoS trust-based routing in delay tolerant networks," *Wireless Personal Communications (Springer)*, June 2011.

[11] J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," *Journal of Network and Computer Applications (Elsevier): Special Issue on Trusted Computing and Communications*, vol. 35, pp. 1001–1012, May 2012.

[12] K. Chan, J.-H. Cho, and S. Adalı, "Composite trust model for an information sharing scenario," *9th IEEE Int'l Conf. on Autonomic and Trusted Computing*, Sept. 2012.

[13] J.-H. Cho, M. Chang, I.-R. Chen, and A. Swami, "A provenance-based trust model of delay tolerant networks," *6th IFIP WG 11.11 Int'l Conf. on Trust Management*, May 2012.

[14] K. Chan and S. Adalı, "An agent based model for trust and information sharing in networked systems," *IEEE Int'l Multi-Disciplinary Conf. on Cognitive Methods in Situation Awareness and Decision Support*, March 2012.

[15] V. Natarajan, S. Zhu, M. Srivatsa, and J. Opper, "Semantics-aware storage and replication of trust metadata in mobile ad-hoc networks," *Proc. 26th IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA)*, March 2012.

[16] C. Castelfranchi and R. Falcone, *Trust Theory: A Socio-Cognitive and Computational Model*. Wiley Series in Agent Technology, 2010.

[17] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," *Proc. IEEE Symposium on Security and Privacy*, pp. 164 – 173, May 1996.

[18] E. M. Uslamer, *Trust, Technology, and Society: Studies in Cooperative Risk Management,*. Earthscan, UK and USA, 2007.

[19] T. C. Earle, M. Siegrist, and H. Gutscher, *Trust in Risk Management: Trust, Risk Perception, and the TCC Model of Cooperation*. Earthscan, UK and USA, 2007.

[20] D. W. Hubbard, *How to Measure Anything: Finding the Value of Intangibles in Business*. John Wiley & Sons, 2010.

[21] M. Delgado, *To Trust or Not to Trust: Ask Oxytocin*. July 2008.

[22] D. S. Alberts and R. Hayes, *Power to the Edge*. DoD Command and Control Research Program, 2003.

[23] K. Chan, R. Pressley, B. Rivera, and M. Ruddy, "Integration of communication and social network modeling platforms using elicit and the wireless emulation laboratory," *Proc. 16th Intl Command and Control Research and Technology Symposium 2011*, June 2011.

[24] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, March 2012.

[25] J.-H. Cho and I.-R. C. Kevin Chan, "A composite trust-based public key management in mobile ad-hoc networks," *ACM 28th Symposium on Applied Computing, Trust, Reputation, Evidence and other Collaboration Know-how (TRECK)*, March 2013.

[26] D. Wynn, M. Ruddy, and M. Nissen, "Tailoring software agents to emulate specific people," in *Proc. 15th Int'l Command and Control Research and Technology Symposium*, June 2010.

[27] J.-H. Cho and K. Chan, "A composite trust based public key management in manets," *6th Annual Network Science Workshop*, April 2012.

U.S. Army Research, Development and Engineering Command

Impact of Trust on Security and Performance in Tactical Networks

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

ICCRTS 2013
Track 1, Paper 065

Kevin Chan, Jin-Hee Cho, Ananthram Swami
US Army Research Laboratory
Computational & Information Sciences Directorate

Outline

- Motivation for trust
- Big questions
- ARL partner programs
- Applications of trust
- Outlook

Motivation

Problem

Enhanced trust can improve decision making, performance, and security, while promoting and maintaining trust in a hostile, dynamic and complex tactical environment is challenging

Objective

Achieve mission/system performance and security requirements

Approach

Develop distributed **trust management** schemes that integrate trust relationships

Payoff

Enhanced Soldier decision making ability

US ARMY RDECOM

Big Questions

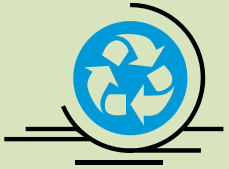
ARL

What is the relationship between trust and security?

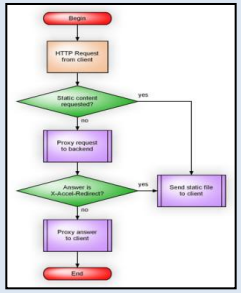
vs.

What does trust bring to security mechanisms compared to existing traditional security mechanisms?

How do we model and measure trust?
How does trust propagate?

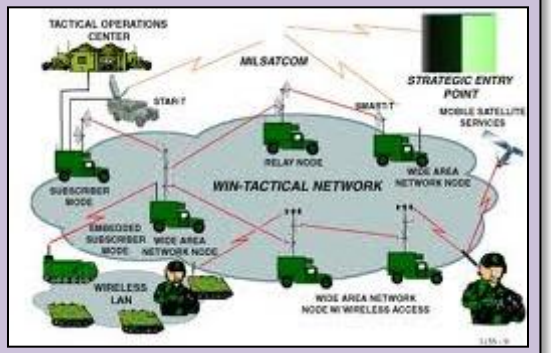


Why is trust useful in tactical networks?
Can we validate trust in tactical networks?



What are the predictors of trust and distrust (whether to trust or cooperate)?

How does trust influence network evolution?
What is the relationship between trust and risk coalition networks?



ARL Partners

Network Science Collaborative Technology Alliance

Understand mathematical principles that govern the co-evolution of information, social-cognitive and communication networks

ns-cta.org

US/UK International Technology Alliance

Develop basic theory behind coalition operations, from a secure networking a decision making perspective

usukita.org

Trust in Networks Claims

- Trust can provide soft metrics to requirements to achieve both security and performance goals
- Concepts and properties of trust can augment existing traditional networking concepts
- Trust is a suitable means to handle interactions between different layers of a multi-genre network
- Trust can augment applications that span the tactical networking space (socio-technical networks)

Traditional & Trust-based Services

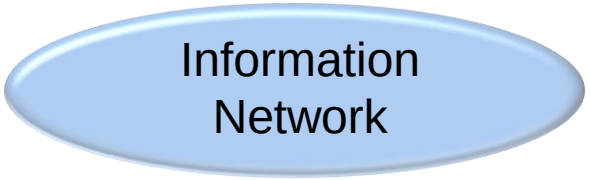
Trust Management Services	Traditional Networking Services
Trust Formation / Update / Propagation	Learning, Refresh
Trust Aggregation	Information/Decision Fusion
Trust Revocation	Access / Key Revocation
Trust Recovery / Repair	Re-entry

Tradeoffs in Trust Management

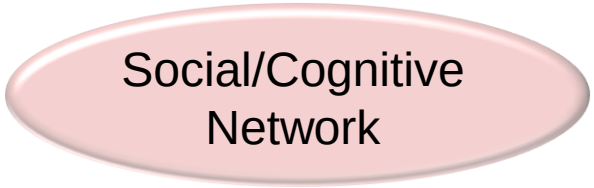
- Trust accuracy vs. Resource Consumption
- Trust vs. Risk (Security)
- Trust vs. Uncertainty

Domain-specific Trust Models

- Trust between nodes
- Dynamics caused by terrain, adversarial actions

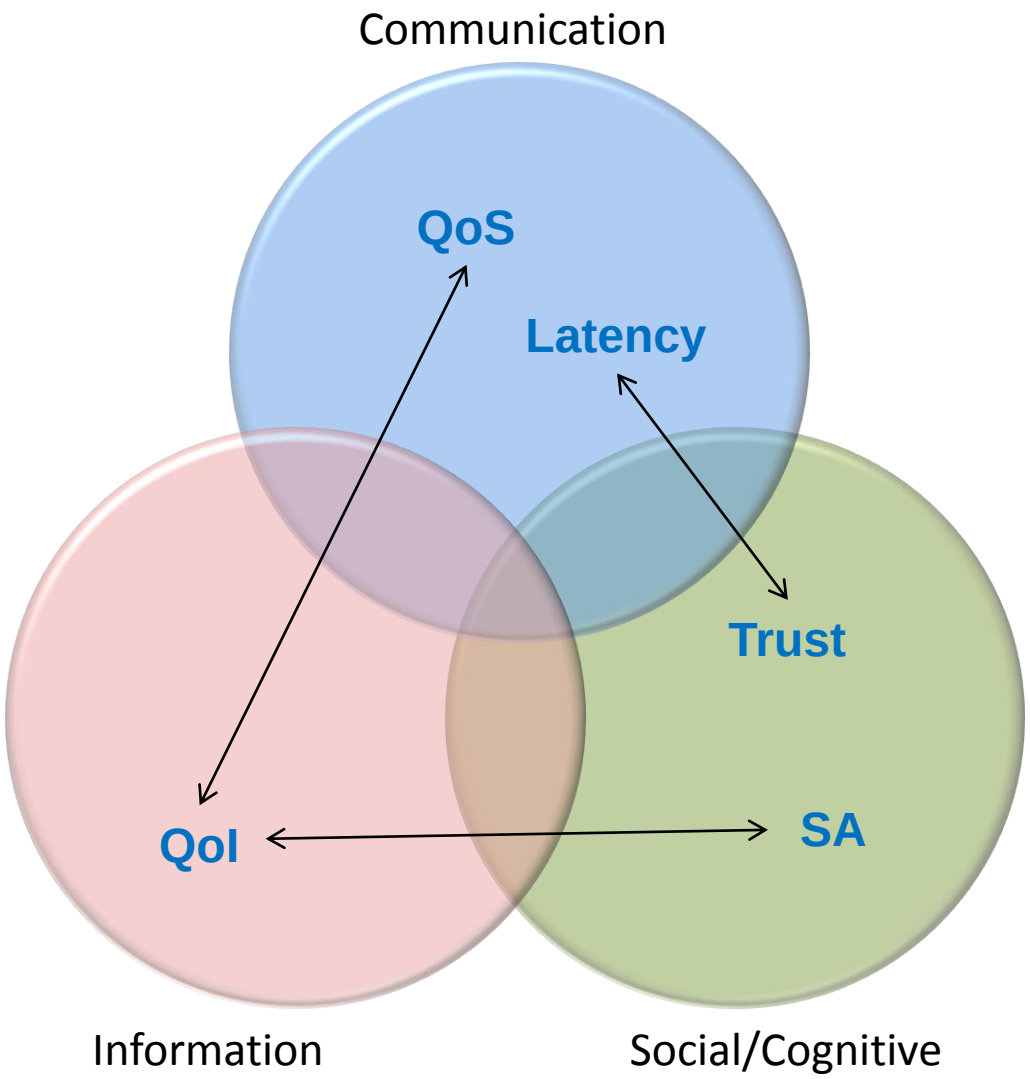


- Trust in information
- Quality of information, provenance, value of information



- Interpersonal trust
- Cognitive processes

Application of Trust to Multi-domain networks



Trust-based Information Sharing in C2

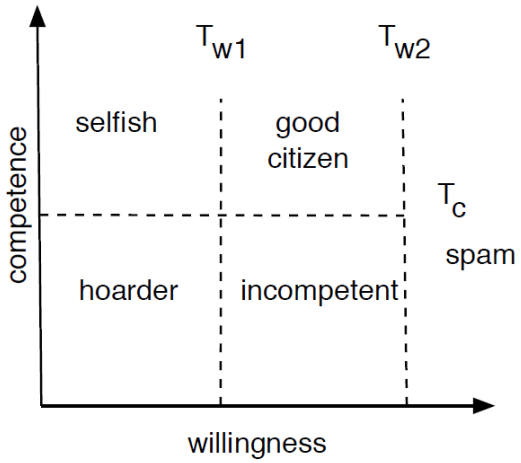
Goal:

- Derive composite trust models for information sharing scenario in C2 environments
- Characterize impact of various behavior of individuals in network on mission performance

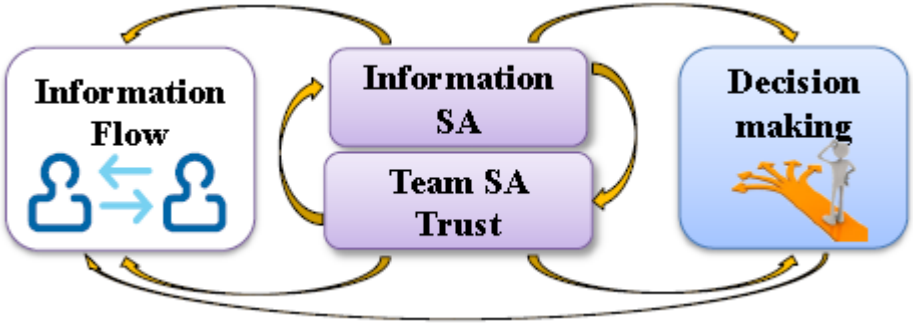
Composite Trust

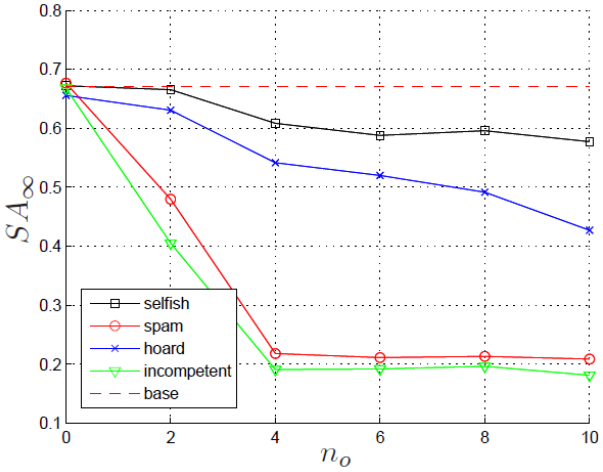
Willingness: behavior in carrying out task

Competence: capability to perform task



Trust based information sharing behavior in C2 scenarios (agent-based ELICIT)





Composite Trust-based Public Key Management

Motivation

- MANET protocol design challenges due to resource constraints and no trusted third party
- Traditional security techniques cannot solve MANET design challenges

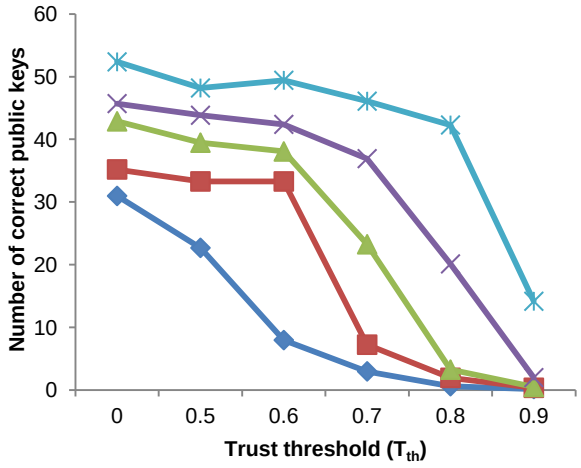
Goal

- Develop a composite trust-based public key management protocol for MANETs
- ***Require high resilience***, ***service provision***, and ***low overhead***, based on the tradeoff between trust and risk

Composite Trust

Integrity | Competence | Social Contact

# of correct public keys in a node grows with lower trust threshold



Result:

An optimal trust threshold can be identified that balances requirements of performance and security

Provenance and Trust Aware Information Fusion

Motivation

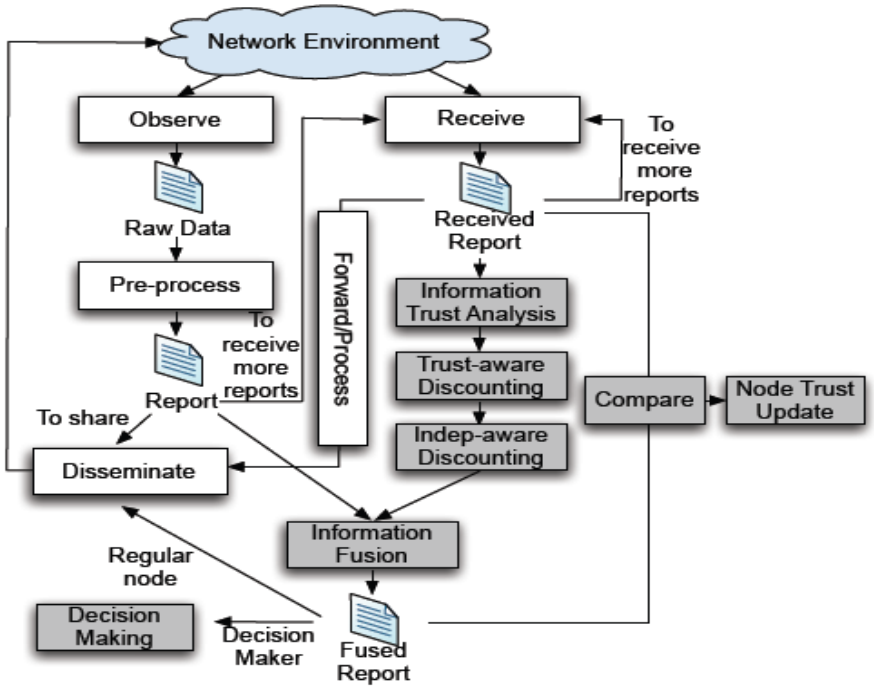
- Trust-based information fusion is critical for effective decision making in dynamic environments
- Existing work investigates "information trust" only based on correctness
- Composite information trust may be needed to filter trustworthy information

Goal

- By applying a *provenance* technique to capture composite information trust, maximize correctness of decision making in a timely manner

Composite Trust

Correctness | *Completeness* |*Timeliness*



Node operations for decision making

Trust-based Security Applications

Threshold of decision making is a *trust vs. risk* evaluation

- **Secure routing**
  - effectiveness for decision making by considering credible information
- **Intrusion Detection**
  - trust threshold to determine a malicious node
  - Social trust that affects detection performance (type I&II errors)
- **Key management**
  - “Soft” approach to PKI, based on a threshold to issue keys

Long-Term Goals

- Trust-based security services that use soft-metrics, but provide equivalent or enhanced security and performance
- Methods to promote trust, control trust within populations / influence behavior
- Models across multi-genre networks that enable prediction of performance metrics not just network quality of service metrics
- Validation of the models with operational scenarios using actual systems and humans-in-the-loop

Thanks!

Questions?

Kevin Chan
US Army Research Laboratory
Network Science Division
kevin.s.chan@us.army.mil